

REMARKS

The Examiner rejected claims 9-13 and 30-34 as being anticipated by US 6,278,783 (Kocher).

The applicant respectfully traverses this rejection.

Kocher is directed towards a masking and permutation scheme for making DES-type cryptography resistant to attack. The scheme involves replacing the key K with a random mask value $K1$ and a masked key $K2$, related to K by the relationship $K2 = K \text{ XOR } K1$. The masked key $K2$ and mask $K1$ are also permuted, with random permutations created $K2P$ and $K1P$.

The message is similarly modified by generating a masked message $M2$ by applying a random value mask $M1$ to the original message M . So, $M2 = M \text{ XOR } M1$. The masked message $M2$ and mask $M1$ are similarly permuted to generate $M1P$ and $M2P$.

The permuted keys and messages are then used, rather than the standard key and message in the cryptographic operation.

See generally column 2 ln 25-66, column 6 ln 29-68 and column 9 ln 1-23.

In Kocher, the masked key $K2$ is the original key K as masked by the random mask $K1$. Conversely, the present application is directed towards a method for split masking. This protects the key mask which is never directly applied to the key. With a split mask, as illustrated for instance in Figure 2 of the present publication, the key mask (equivalent to $K1$) is never applied directly to the key K .

Kocher appears to be a variant of the Messerges method described at paragraph [0008] of the published application. In the Kocher variant, the plaintext input is also masked, with $M1$, and both the masked input $M2$ and the masked key $K2$ are permuted.

Figure 1 of the published application illustrates the prior art, a key applied to a plaintext.

Figure 2 of the published application illustrates the split masking method that may be contrasted with Kocher in a number of ways. First, there is no permutation specified in the present application. Second, the operation $K2 = K \text{ XOR } K1$ is never directly computed. Third, split masks are applied to the key K , not a single mask $K1$.

To summarise the differences, Kocher is directed towards disguising the key by masking the key (K) with a single key mask ($K1$) and permuting the resultant. Kocher is trying to protect the key at a different point in the process and does not address the vulnerability that is the focus of the present application. Kocher does not disclose a method to protect K , $K1$ or $K2$ during the operation $K2 = K \text{ XOR } K1$. Kocher does not disclose the use of split masks or applying split mask values to a key. Kocher does not disclose defining a value mn as currently claimed.

The present application, conversely, is directed towards protecting the masking operation and the mask being applied by indirectly applying a mask to the key using split masks. By using split masks, the mask is never directly applied to the key.

The presently considered claims have several features different from Kocher including: a set of n random input values; defining a masked function by masking the defined cryptographic function with the value $m_{in1} \wedge \dots \wedge m_{inn}$; obtaining a set of random values m_1, \dots, m_{n-1} ; defining a value m_n to be $r \wedge m_{in1} \wedge \dots \wedge m_{inn} \wedge m_1 \wedge \dots \wedge m_{n-1}$; and using the values m_1, \dots, m_n and m_{key} to define input. None of these features are disclosed in Kocher. The applicant has reviewed the sections cited by the Examiner and disagrees that Kocher discloses these features.

The applicant requests that the Examiner withdraw this objection.

Favourable reconsideration and allowance of this application are respectfully requested.

A Petition for an Extension of Time requesting an extension of one month for filing the subject response is enclosed. The Commissioner is authorized to charge any deficiency or credit any overpayment in the fees for same to our Deposit Account No. 500663.

Executed at Toronto, Ontario, Canada, on March 25, 2009.

CATHERINE HELEN GEBOTYS

By: 

Etienne de Villiers

Registration No. 58632

(416) 971-7202, Ext. 300

Customer Number: 38735

EDEV

Atts. Petition for Extension of Time